

Analytical Brief

Regulation of Artificial Intelligence: EU Experience and Future Regulation in Ukraine

December 2025

Stanislav Yukhymenko



Author: Stanislav Yukhymenko, Research Fellow at IER

This material was prepared within the framework of the project "Assessment of the Economic Impact of EU Law Adaptation on Selected Sectors of Ukraine's Economy" with support from the European Union and the International Renaissance Foundation as part of the joint initiative "Joining the EU Together". The material represents the authors' position and does not necessarily reflect the position of the European Union or the International Renaissance Foundation.

© Institute for Economic Research and Policy Consulting, 2025



Introduction

In July 2024, the European Union launched a global experiment in the regulation of artificial intelligence. Regulation (EU) 2024/1689¹ became the world's first comprehensive legislative act establishing mandatory rules for developers and users of artificial intelligence systems. This step marks a transition from voluntary ethical principles to legally binding norms, compliance with which will become a condition for access to the European market.

For Ukraine, the issue of artificial intelligence regulation extends far beyond purely technical matters. After obtaining candidate status for EU accession in 2022 and the commencement of membership negotiation processes, Ukraine is obligated to align its legislation with the EU's *acquis communautaire*. The AI Act is part of this *acquis*, and therefore its implementation is not a matter of choice, but rather a question of pace and sequence of harmonization. Ukraine's accession to the European Council on Artificial Intelligence in October 2025 became the first institutional step in this direction.

At the same time, the EU itself is restructuring its approach. After the adoption of the AI Act, it became evident that the ambitious implementation timeline and delays with technical standards create significant risks for businesses. Against this backdrop, the European Commission is considering options to adjust the pace of introducing requirements to avoid losing competitiveness.

The purpose of this document is to analyze the regulatory architecture of the AI Act and related EU acts, assess European businesses' responses to the new regulation, and identify potential opportunities and challenges for Ukraine in aligning with these standards. The document offers recommendations for crafting a balanced policy that balances fulfillment of integration obligations with support for the Ukrainian AI sector.

Regulatory Architecture of the European Union

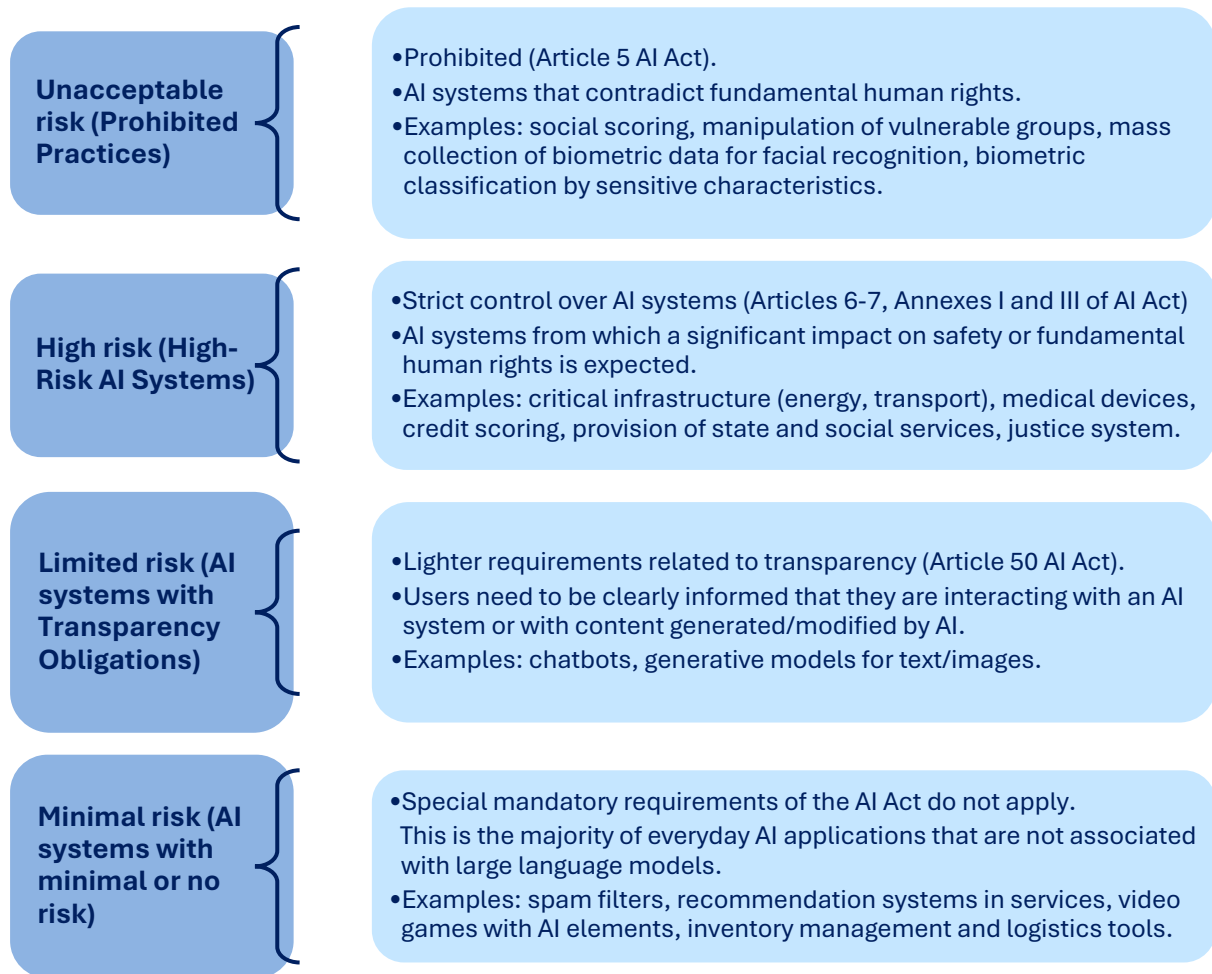
Risk Categories

The AI Act, which entered into force on August 1, 2024, introduces a comprehensive regulatory framework for AI in the European Union. At its core is the classification of AI applications by risk level. The Regulation divides AI systems into several categories, each with a different regulatory regime. In other words, the higher the potential risk posed by a specific AI system, the stricter the requirements and restrictions imposed on it. Based on the provisions of the AI Act, four primary risk categories are identified².

¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

² European Commission. (2024). Regulatory framework for Artificial Intelligence, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Fig. 1. Main AI risk categories



Source: based on the AI Act and analysis by the Future of Life Institute³

Unacceptable risk (Prohibited Practices, Article 5 AI Act) refers to uses of AI that by their nature contradict fundamental principles and rights. This category includes, in particular, social scoring (evaluating a person based on behavior or characteristics), algorithmic systems for manipulating human behavior, and real-time biometric identification systems for people in public places (such as facial recognition).

High risk (High-Risk AI Systems, Articles 6-7, Annexes I and III of the AI Act) refers to uses of AI that are expected to have a significant impact on safety or fundamental human rights. The Regulation contains a list of areas where AI is considered high-risk (Annex III⁴ to the Regulation), including: critical infrastructure, education and training, employment (personnel selection and evaluation), management of databases and services of general use, law enforcement, and justice. High-risk AI systems are permitted but placed under strict control: requirements for safety, data quality, and transparency; mandatory human

³ Future of Life Institute, High-level summary of the AI Act, <https://artificialintelligenceact.eu/high-level-summary/>

⁴ Annex III to Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng#anx_III

oversight of their operation; and conformity assessment before market launch and throughout the product lifecycle. Developers of such systems must conduct evaluations of their impact on fundamental human rights, document and trace algorithmic operations, ensure appropriate cybersecurity, ensure the ability to explain results, and so on.

Limited risk (Systems with transparency obligations, Article 50 AI Act) refers to uses of AI that do not belong to the first two categories but can still affect users. The Regulation defines transparency requirements for them: for example, systems that generate content (texts, images, videos), or chatbots. They must inform the user that they are interacting with AI, or that the content was created artificially.

Minimal risk encompasses all other uses of AI that do not pose significant threats. The AI Act does not establish any special requirements for them, effectively allowing unrestricted use. This includes most household and office applications of AI, such as spam filters in email, product recommendation algorithms, AI in games (like Stockfish in chess, which is a highly specialized tool and not suitable for anything other than playing chess), and so on. The "Minimal risk" category is not found in the AI Act but appears in EU communications. Presumably, this category is not mentioned directly in the regulation because these AI systems are relatively well-prepared algorithms not based on large language models.

Separately, the AI Act (Chapter 5) identifies the concept of **General-Purpose AI (GPAI)**. These are artificial intelligence models with a wide range of applications that can perform various tasks and be used in different fields without a narrow initial specialization. A typical example is large "foundation" models like GPT-5, Gemini, or similar generative models capable of producing text, images, or videos in response to arbitrary requests. The emergence of such systems during the preparation of the AI Act (the generative AI boom in 2022–2023) prompted⁵ the addition of a special regime for them, since under the classic risk assessment scheme, they did not fit directly into any category.

Providers of GPAI models (those who develop and release foundation models to the market) have separate transparency and safety obligations (Article 53, Annexes 11-12 AI Act). In particular, they must document technical information about the model and provide it to supervisory authorities upon request; ensure a copyright compliance policy (so that data for training models does not violate rights holders' rights); and publish a summary report on the training data used (a generalized description of the datasets).

The AI Act in Article 113 introduces a phased timeline for the application of its provisions:

- **February 2, 2025:** Prohibitions on AI systems with unacceptable risk enter into force (Chapters I-II);
- **August 2, 2025:** Obligations for general-purpose AI (GPAI) models come into effect, and Member States must designate national competent authorities (Chapter III, Section 4, Chapters V, VII, and XII);
- **August 2, 2026:** The Regulation begins to apply in full scope for most high-risk

⁵ «What is the EU AI Act and when will regulation come into effect?» Reuters, December 6, 2023. <https://www.reuters.com/technology/what-are-eus-landmark-ai-rules-2023-12-06/>

systems, and national regulatory sandboxes must become operational (a controlled environment where companies can test innovative AI systems and receive clarification on regulatory expectations without the risk of immediate penalties from the regulator);

- **August 2, 2027:** The final obligations for specific categories of embedded high-risk systems (for example, in medical devices) enter into force (Article 6(1) and corresponding commitments).

Institutional Architecture

A new institutional system of oversight and enforcement is being created to implement the AI Act, described in detail in Chapter VII of the regulation. It essentially resembles the mechanism introduced in the EU for data protection (GDPR), but has its own specific features.

Each EU Member State must designate one or more AI supervisory authorities responsible for enforcing the regulation at the national level. These may be completely new structures or expanded powers of existing ones – for example, product certification bodies, cybersecurity agencies (like CERT-UA), or other government bodies related to digital transformation. The main thing is that they have sufficient expertise and resources in AI. These competent authorities will register providers of high-risk systems, monitor that they undergo conformity assessment before market launch, conduct market surveillance (i.e., check already deployed systems for compliance with requirements), consider complaints from users or civil society organizations, and apply sanctions when violations are detected.

The **European Artificial Intelligence Board** (Article 65 AI Act) is an EU coordination body that will bring together representatives of all national regulators and the European Commission. Its task is to ensure the consistent application of the AI Act throughout the Union. The Board will develop recommendations and guidance clarifications on the practical implementation of the law, and exchange information about new risky practices. The AI Board should help avoid regulatory fragmentation and discrepancies between countries. The European Commission will provide the secretariat of this body. Ukraine has already joined the European Artificial Intelligence Board.⁶

EU AI Office (Article 64 AI Act). This is the central "techno-regulator" within the European Commission's structure, which directly supervises the most powerful general-purpose AI (GPAI) models. The AI Office has the authority to conduct assessments, demand information from developers, and impose hefty fines. The AI Office was created within the structure of the European Commission as a central element of the AI Act governance system, which will perform the functions of the secretariat of the AI Board, as well as certain central functions – in particular, maintaining the European register of high-risk AI systems, receiving reports on serious incidents from providers, and administering voluntary codes that companies are willing to voluntarily comply with (such as the GPAI

⁶ "Ukraine joined the European Artificial Intelligence Board." Press Service of the Cabinet of Ministers of Ukraine, October 31, 2025. <https://www.kmu.gov.ua/news/ukraina-pryiednalasia-do-ievropeiskoi-rady-zi-shtuchoho-intelektu>

code⁷ in the EU and the Voluntary Code for Responsible Use of Artificial Intelligence in Ukraine).⁸

According to Article 70 of the AI Act, at the national level, each Member State must establish or designate at least one "notifying authority" and one "market surveillance authority."

The **Notifying Authority (Article 28 AI Act)** is a national body responsible for accrediting and designating conformity assessment bodies (Notified Bodies) for high-risk AI systems, as well as supervising their activities. In other words, the notifying authority does not itself certify AI systems, but issues notifications (authorizations) to specialized institutions that will conduct conformity assessment (audit, testing, certification) of AI systems covered by the AI Act. Ukraine, for European integration, must also determine who will perform this function. Presumably, this could be the National Accreditation Agency of Ukraine or a new certification body.

Notified Bodies are organizations independent from AI model manufacturers, officially designated by national notifying authorities to conduct conformity assessment of high-risk AI systems. They verify technical documentation, manage risk, and implement quality models; test systems for compliance with safety requirements; and assess continuous compliance throughout the AI lifecycle.

Since the AI Act recently entered into force, the official list of "Notified Bodies" specifically for the AI Act is still in the formation stage. The following companies may likely be included:

- BSI (British Standards Institution). They have a Dutch division (BSI Group The Netherlands B.V.) actively working to obtain Notified Body status for the AI Act and have a Head of AI Notified Body on staff.⁹
- TÜV SÜD. These are German giants in testing, inspection, and certification (TIC). They are already Notified Bodies for other EU directives.¹⁰
- SGS (Société Générale de Surveillance). They are a leading Notified Body headquartered in Switzerland, which has accredited bodies throughout the EU for medical devices, radio equipment, and cybersecurity.¹¹

⁷ The General-Purpose AI Code of Practice, prepared by the European Commission. <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpaid>

⁸ "Voluntary Code of Conduct for Ethical and Responsible Use of Artificial Intelligence" – Ukraine. <https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%94%D0%BE%D0%B1%D1%80%D0%BE%D0%B2%D1%96%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%20%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D1%96%D0%BD%D0%BA%D0%B8.pdf>

⁹ Notifications – NANDO / Single Market Compliance Space (SMCS), BSI Group The Netherlands B.V., https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies/notifications?organizationRefCd=NANDO_INPUT_243705

¹⁰ Notifications –NANDO / Single Market Compliance Space (SMCS), TÜV SÜD Product Service GmbH, https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies/notifications?organizationRefCd=EPOS_43445

¹¹ SGS – «Data & Artificial Intelligence» (Service Group). <https://www.sgs.com/en-de/service-groups/data-and-artificial-intelligence>

The **market surveillance authority** is the primary national body responsible for implementing the AI Act. Its key function is to monitor AI systems already on the market to ensure their compliance with the AI Act. This body investigates cases of noncompliance and is endowed with broad powers: it can demand access to technical documentation, source code, require corrective actions, impose fines, and prohibit systems it considers dangerous.

Separately, the AI Act obliges each state to determine which national public bodies are responsible for ensuring compliance with fundamental human rights requirements when using high-risk AI systems. This concerns areas where AI is used to make decisions about people – for example, candidate selection for employment, creditworthiness assessment, education systems, law enforcement, etc. The AI Act does not create new human rights institutions. Still, it requires countries to designate which national regulators or supervisory bodies will monitor whether the application of AI does not violate fundamental rights.

The AI Act encourages Member States to create environments for the pilot implementation of AI – so-called regulatory sandboxes, where companies, with the assistance of the regulator, can test their innovative systems and gradually bring them into compliance with the law. It is expected that such pilot regimes will help reduce the risks associated with AI products and, at the same time, provide regulators with a better understanding of the technologies. Ukraine, by the way, is already adopting this idea: the Ministry of Digital Transformation announced¹² the creation of an AI sandbox aligned with European norms, where domestic companies will be able to voluntarily test their developments in line with the requirements of future EU law. In Ukraine, the opportunity to submit applications to the regulatory sandbox organized by the Ministry of Digital Transformation in cooperation with the Innovation Development Fund has already been opened.¹³

Connection with Other EU Laws

Digital Services Act (DSA)¹⁴ – the Act on Digital Services (entered into force in 2022, main provisions apply from 2023–2024). This regulation establishes rules for online platforms and services regarding content moderation, transparency of algorithms and advertising, user protection, etc. The DSA obliges very large online platforms (such as social networks and search engines) to disclose their recommendation system policies, conduct risk assessments of their algorithms for society, provide access to data for audits, etc. Although the DSA is not directly aimed at AI, it regulates the use of AI algorithms on platforms. For example, content recommendation systems must be transparent to users (they must explain on what basis something is being offered to them) and be subject to checks by independent experts.

¹² "Ukraine announced the launch of a regulatory 'sandbox' for artificial intelligence developers." Center for Democracy and Rule of Law (CEDEM), March 29, 2023. <https://cedem.org.ua/news/regulyatorna-pisochnytsia/>

¹³ "Sandbox for AI and Blockchain Startups" – Ukrainian Startup Fund (program). <https://usf.com.ua/programs/sandbox-ai-blockchain-startups>

¹⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>

Data Act¹⁵ (adopted in 2023, entered into force in January 2024, will apply from September 2025) establishes rules regarding data sharing between companies, user access to data generated by their devices (especially smartphones), data portability when changing cloud service providers, conditions for government access to business data in exceptional cases, etc. In the AI field, the Data Act is of great importance, as training AI models depends on the availability of large datasets.

The **General Data Protection Regulation** (GDPR¹⁶), in effect since 2018, is one of the most well-known EU laws, establishing strict requirements for the processing of personal data. Artificial intelligence very often works with data about people; therefore, all AI systems that process personal data must also comply with GDPR norms.

Stakeholder Reactions in the EU

The introduction of the AI Act triggered an active reaction from stakeholders — from large technology companies and business associations to civil society organizations and academics.

Most European business associations generally support the goals of the EU's Artificial Intelligence Act (AI Act) – increasing trust in AI and unifying rules in the common market. The tone of their reaction is predominantly constructive: business approves of the risk-based approach and the EU's aspiration to become a leader in "trustworthy AI," but with numerous comments and warnings. Companies and associations from various countries emphasize that the law must be implemented carefully to avoid stifling innovation and overburdening businesses with excessive requirements.

Positions of Key European Business Associations

- BusinessEurope (a pan-European business confederation) supports the creation of a European "rulebook" for AI, but warns against haste and ill-considered decisions. Emphasizes the need to define scope and timelines precisely before introducing requirements. BusinessEurope supports the risk-based regulatory model but criticizes overly broad coverage (especially regarding "General Purpose AI") and the imposition of liability alongside other acts.¹⁷
- DIGITALEUROPE (pan-European association of IT/tech companies) supports the goals of the AI Act regarding "trust based on risks" and the balance of rights and innovation. It welcomes the fact that regulators tried to balance safety and rights protection with the competitiveness of the AI industry; however, it criticized the final

¹⁵ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>

¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

¹⁷ https://www.besnesseurope.eu/wp-content/uploads/2025/02/2023-11-30_besnesseurope_ai_act_statement-1a4-1.pdf

compromise for "turning upside down" the risk-based approach by hasty additions of strict requirements for foundation models.¹⁸

- SMEUnited (the association of small and medium-sized enterprises of the EU) supports the goals of the AI Act but emphasizes proportionality for SMEs. SMEUnited has repeatedly called on legislators to take into account the limited resources of small businesses, simplify compliance requirements, and prevent a situation in which only large players can "afford" to comply with the regulation. The association welcomed the latest proposed changes from the European Commission.¹⁹
- German business supports unified rules but insists on a narrow definition of AI, the introduction of a "significant risk" criterion, harmonization with sectoral norms, and realistic requirements; Germany, together with France, lobbied to soften GPAI regulation to protect its developers.²⁰
- French business supports AI regulation, but insists on investments and conditions that will allow the development of "European AI"; MEDEF and startup associations emphasize the need for incentives and flexible implementation, and France, together with Germany, advocated for softening requirements for GPAI to support local companies like Mistral AI.²¹

As for the tech giants from the USA, they also actively lobbied for their interests. OpenAI, Google, Microsoft, and others tried to influence the wording regarding GPAI and high risk. In particular, Sam Altman (OpenAI) initially sharply criticized the early draft of the law, even threatening to exit the EU market, but later softened his position.

"Digital Omnibus": Strategic Retreat for the Sake of Competitiveness

On November 19, 2025, the European Commission published a package of legislative initiatives called the Digital Omnibus.²² This document acknowledged that the original implementation timeline for the AI Act is unrealistic and threatens the competitiveness of European businesses.

The key factor was the delay in developing harmonised standards. The CEN and CENELEC organizations did not manage to prepare technical specifications that serve as the basis for the "presumption of conformity." Without these standards, companies

¹⁸ "'A text we can work with': Reaction to European Parliament vote on the Regulation (EU) 2024/1689 (AI Act)" — DIGITALEUROPE, June 14, 2023. <https://www.digitaleurope.org/news/a-text-we-can-work-with-reaction-to-european-parliament-vote-on-ai-act/>

¹⁹ <https://www.eubusiness.com/sme/smeunited-digital-package-sme-readiness/>

²⁰ <https://www.bitkom.org/EN/List-and-detailpages/Publications/Position-on-EU-Artificial-Intelligence-Act-trilogue-negotiations>

²¹ <https://medef-aisne.fr/fr/actualite-nationale/ia-10-propositions-pour-reussir>

²² Digital Omnibus – Proposal for a Regulation on simplification of the digital legislative framework (COM(2025) 837 final, 19 November 2025). Brussels, 2025, <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>

would face legal uncertainty, risking fines for noncompliance with requirements whose technical implementation is undefined.

Key Changes to the Implementation Timeline According to the Omnibus²³:

- High-risk systems (Annex III): The initial deadline (August 2, 2026) is postponed. The new deadline is December 2, 2027 (6 months after the official approval of the standards). This gives businesses an additional 16 months for preparation.
- Integrated systems (Annex I): For AI that is a safety component of regulated products (medical devices, automobiles, elevators), the deadline is postponed to August 2, 2028.
- Simplification for SMEs: The Omnibus removes companies' direct obligation to ensure "AI literacy" for personnel, transferring responsibility for education to Member States. Simplified technical documentation for small and medium-sized enterprises is also being introduced.

Overall, the EU's strategy is evolving from a "regulation first" approach to seeking a more flexible balance. If the 2024 proposals focused more on protecting human rights and safety, the European Commission's new 2025 proposals are characterized by a pragmatic course correction against the backdrop of fierce global competition in artificial intelligence. A year after adopting the AI Act, Europe realized that excessive regulation could weaken its technology sector, putting it at a disadvantage in competition with the USA and China. The EU competitiveness report, chaired by Mario Draghi,²⁴ became a catalyst for change, calling for a transition from "regulation at any cost" to "simplification for the sake of innovation."

Specifics of AI Use in the Military Sphere

The AI Act, under Article 2, states that it does not apply to systems that are part of weaponry or used exclusively for defense purposes. This decision was made because defense and national security issues are considered the sovereign right of each EU member country. At the same time, a complex situation arises with dual-use technologies. If an AI system (for example, an object recognition system for satellite images) was created for the civilian market and later used solely for military purposes without modification, it falls outside the scope of the AI Act. However, if it is used simultaneously for both civilian (e.g., police officers) and military purposes, its civilian application falls under regulation.

²³ Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation, Press release, European Commission, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718

²⁴ The future of European competitiveness: Report by Mario Draghi, European Commission, 2024, https://commission.europa.eu/topics/competitiveness/draghi-report_en

Despite the exception in the AI Act, the European Parliament takes an active position on restricting military AI. The European Parliament, in its Resolution²⁵ of September 12, 2018, regarding autonomous weapons systems, called for the development and conclusion of an international treaty prohibiting lethal autonomous weapons systems (LAWS). The experience of using AI technologies during the Russo-Ukrainian war will likely significantly influence future international legislation on the military use of AI.

The European Parliament's key requirement is ensuring "meaningful human control" over all weapons systems.

This means that a human must always have the ability to make the final decision on the use of lethal force. Here, the question arises of the degree of human involvement, and whether the level of human involvement in managing AI-equipped means currently in the Ukrainian armed forces will be acceptable.

Regulation of AI in Ukraine

Ukraine, as a candidate state for EU accession, is aligned with European approaches to regulating the digital sphere, including artificial intelligence. Although there is no specific law on AI in Ukraine yet, several steps have been taken in recent years to develop a policy for the development and use of AI technologies.

The first fundamental document was the Concept for the Development of Artificial Intelligence in Ukraine²⁶, approved by the Cabinet of Ministers in December 2020. It outlined the general vision of state policy in this area: to promote the development of AI to safeguard citizens' rights and needs, strengthen the economy, and improve public administration. The Concept identified nine priority areas — education, science, economy, cybersecurity, defense, information security, public administration, legal regulation and ethics, and justice.

In autumn 2023, the Ministry of Digital Transformation presented a "roadmap"²⁷ for AI regulation, outlining general plans for further regulation of the AI sector. This was elaborated in more detail in June 2024 in the document "White Paper on AI Regulation in Ukraine: Ministry of Digital Transformation's Vision."²⁸ This analytical material outlines what the government considers the optimal path for implementing AI regulation. Importantly, this is not a normative act, but a document for consultation – it was put up for discussion with all stakeholders.

²⁵ European Parliament Resolution P8_TA(2018)0341 of 12 September 2018 on autonomous weapon systems. Doceo document, European Parliament. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html

²⁶ Order of the Cabinet of Ministers of Ukraine "On approval of the Concept for the Development of Artificial Intelligence in Ukraine" No. 1556-r of 02.12.2020. <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>

²⁷ "Regulation of artificial intelligence in Ukraine: presenting the roadmap" – Ministry of Digital Transformation of Ukraine, October 7, 2023. <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu>

²⁸ "Regulation of artificial intelligence in Ukraine: presenting the White Paper" – Ministry of Digital Transformation of Ukraine, June 26, 2024. <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-bilu-knigu>



The "White Paper" proposes a two-level strategy that will allow Ukraine to gradually adapt to the new rules.

In the first stage, it is planned to implement several non-legislative, predominantly voluntary, instruments:

- regulatory sandbox: creating a safe environment for companies where they can test their AI products under state supervision. This will help developers immediately take into account future AI Act requirements and facilitate entry to the EU market;
- methodology for assessing AI impact on human rights: development of a Ukrainian methodology that companies can voluntarily apply to analyze the risks of their systems;
- AI content labeling: creation of recommendations and tools for marking AI-generated content;
- voluntary codes of conduct: development of ethical rules for various sectors (medicine, finance) that use AI.

After completing the preparatory stage and collecting feedback, the Ministry of Digital Transformation plans to draft a law on AI. It is expected that this law will be maximally harmonized with the European AI Act.

Potential Benefits of Alignment with the AI Act for Ukraine

1. Single digital market and export opportunities. Compliance with AI Act norms will become a prerequisite for mutual recognition of Ukrainian AI products in the EU. This will open access to the European market for our companies without additional barriers. In fact, an AI product certified in Ukraine can be freely sold in the EU – and vice versa. Such integration will promote the growth of IT exports and attract investments in high-tech sectors.
2. Acceleration of digital integration into the EU. The AI Act is part of a broader package of EU digital legislation. On the path to EU membership, Ukraine is obligated to adopt the EU's *Acquis Communautaire*. Negotiations can only concern the duration of transition periods.
3. Long-term economic effect. Although in the short term there will be costs associated with compliance with the rules, in the long term, economic returns are expected. According to European Commission estimates, a common regulatory framework for AI could add nearly EUR 295 bn to Europe's GDP and create 4.6 million new jobs by 2030.²⁹ Ukrainian companies can share in this growth if they integrate into the European market.

²⁹ Evas, T. (2020). European framework on ethical aspects of artificial intelligence, robotics and related technologies. European Parliamentary Research Service (EPRS), [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2020\)654179](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)654179)

Main Challenges and Risks

The main financial burden will fall specifically on Ukrainian companies, primarily on the technology sector, which is one of the drivers of the economy. Costs can be divided into several key categories, similar to those faced by businesses in the EU.

Direct compliance costs. Ukrainian developers planning to work in the EU market will have to bear the full range of expenses incurred by AI system providers. The analytical center Centre for European Policy Studies (CEPS) in 2021 estimated³⁰ the scope of costs that AI developers in the EU face:

- **Creation of quality management systems (QMS),** which includes the development of internal procedures to ensure compliance of each AI product with AI Act requirements at all stages – from model design to market monitoring. Companies that will work with high-risk AI products will have to prepare extensive documentation: descriptions of the architecture and algorithms, reports on the data used, risk assessment methods, and test results.³¹ If the company did not previously have a QMS (typical for startups), according to CEPS estimates, the costs of creating an entirely new QMS can reach EUR 200–330 thous. one-time, plus about EUR 70 thous. annually for maintenance.
- **Audit and certification:** The cost of certifying one high-risk AI system with a European notified body is estimated at EUR 17–23 thous. on average. This does not include internal costs for documentation preparation and testing, which can reach hundreds of thousands of euros, depending on the product's complexity.
- **Technical adaptation of models:** Companies will have to invest engineering resources in checking and cleaning datasets for bias, implementing mechanisms for explaining AI decisions, and strengthening cybersecurity. These are mainly costs for paying highly qualified engineers.
- **Legal support:** Engaging external consultants to interpret AI Act requirements can cost from several thousand euros per consultation to hundreds of thousands of euros for full project support.³²

It is worth noting that some AI developers may already have a quality management system that meets EU requirements, and therefore, they will not have to spend resources on this again.

The Ukrainian IT sector primarily consists of small and medium-sized companies and startups. It is for them that the AI Act requirements can become a threat. According to

³⁰ "Clarifying the costs for the EU's AI Act" – Centre for European Policy Studies (CEPS), September 24, 2021. <https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/>

³¹ Article 16 – "Obligations of providers of high-risk artificial intelligence systems" Regulation (EU) 2024/1689. <https://artificialintelligenceact.eu/article/16/>

³² DIGITALEUROPE. (2025). The Executive Brief: Removing regulatory burden for a more competitive and resilient Europe. <https://cdn.digitaleurope.org/uploads/2025/09/DIGITALEUROPE-THE-EXECUTIVE-BRIEF.pdf>

CEPS estimates, SMEs can incur costs of up to EUR 400,000 to bring one high-risk product to market if they do not have well-developed quality management systems. Their costs in Ukraine will likely be somewhat lower due to lower certification service costs. At the same time, tiny Ukrainian AI startups planning to develop projects in areas the EU considers high-risk, such as medicine, fintech, education, and personnel work, will not be able to finance the necessary measures.

Although the AI Act provides for SME support measures (regulatory sandboxes, reduced fees), the main costs for process development and technical adaptation remain. The size of Ukrainian startups is predominantly much smaller than in the EU, and therefore, the costs of complying with all AI Act and GDPR requirements can halt a startup's life at the idea stage.

Currently, the Ukrainian artificial intelligence sector is entering the implementation phase of the AI Act, one of the most dynamic in Central and Eastern Europe. As of 2024-2025, there are 243 companies in Ukraine specializing in AI.³³ This indicator places Ukraine second in the region, behind only Poland, where 301 such companies are registered.

The Ukrainian AI market is estimated at USD 419.4 m in 2025.³⁴ This market is supported by qualified workers: the total number of AI/ML specialists reached 5,200 as of January 2024.³⁵

If we assume that 10-15% of Ukrainian AI companies will develop high-risk AI models, the total business costs of meeting all AI Act requirements will be measured in the tens of millions of euros over the next 3-5 years.

But the most important thing will not be the total cost. High regulatory costs, combined with the small size of Ukrainian AI startups, can pose a significant barrier to projects in industries the AI Act defines as high-risk, namely medicine, education, and infrastructure.

Ukrainian startups developing AI systems for high-risk areas will need additional support, as it is for such systems that the AI Act establishes the strictest requirements – in particular, the presence of a quality management system, detailed technical documentation, and monitoring procedures.

Large IT companies that already work with clients in the EU will likely adapt faster: many already have elements of quality management, information security, and compliance in place, as such requirements are often included in contracts or industry standards. However, they will also have to adjust internal processes, as full compliance with the AI Act requires adherence to specific requirements for high-risk AI systems.

³³ "WINWIN AI Center of Excellence – Digital Development and Innovation Strategy until 2030" – Ministry of Digital Transformation of Ukraine, https://winwin.gov.ua/assets/files/%D0%A3%D0%9A%D0%A0%20WINWIN_AI_1.pdf

³⁴ "WINWIN AI Center of Excellence – Digital Development and Innovation Strategy until 2030" – Ministry of Digital Transformation of Ukraine, https://winwin.gov.ua/assets/files/%D0%A3%D0%9A%D0%A0%20WINWIN_AI_1.pdf

³⁵ "AI Ecosystem of Ukraine: talents, companies, education" – AI HOUSE (in collaboration with Roosh), June 2024. <https://aihouse.org.ua/wp-content/uploads/2024/01/AI-Ecosystem-of-Ukraine-by-AI-HOUSE-x-Roosh-UA.pdf>

Conclusions and Recommendations

The European AI Act is establishing a new regulatory paradigm in which access to the EU market is conditioned on compliance with requirements on safety, transparency, and the protection of human rights.

The analysis revealed several key patterns:

- First, the EU itself is in the process of calibrating its approach: delays in developing standards and the "Digital Omnibus" proposals indicate that the initial regulatory ambitions have encountered practical limitations. This opens a window of opportunity for Ukraine to implement more balanced policies.
- Second, European business generally supports the AI Act's risk-based approach, but consistently points to the threat of excessive regulatory pressure on competitiveness.

For Ukraine, alignment with EU standards is simultaneously an integration obligation and a strategic choice that will determine the country's positioning in the global artificial intelligence technology market.

For the Ukrainian AI sector, comprising over 240 companies and more than 5,000 specialists, alignment with the AI Act presents both opportunities and challenges. On the one hand, harmonization opens access to the European market and increases international partners' trust in Ukrainian developers. On the other hand, compliance costs for high-risk systems can reach hundreds of thousands of euros per product, which constitutes a significant barrier for startups.

Based on the conducted analysis, the following steps are recommended:

- In the area of legislative harmonization, it is recommended to continue preparing the law on artificial intelligence, taking into account the current changes to the AI Act proposed by the "Digital Omnibus." It is advisable to avoid the preemptive implementation of provisions that have not yet entered into force in the EU.
- In the area of institutional development, after the adoption of appropriate legislation, it is necessary to designate a national authority for AI market surveillance and an authority for notification and accreditation of conformity assessment bodies.
- In the area of business support, it is necessary to ensure the full functioning of the AI regulatory sandbox. Simplified technical documentation templates in Ukrainian should be developed, and a program for partial reimbursement of certification costs for SMEs developing high-risk AI systems should be considered.
- In the area of international cooperation, it is recommended to actively participate in the European Artificial Intelligence Board to exchange experience and influence the development of AI Act application practices. It is also advisable to establish cooperation with European notified bodies to train Ukrainian specialists in conformity assessment.

With a balanced approach, alignment with European AI regulatory standards can not only fulfill integration obligations but also catalyze the growth of the technology sector.



Institute for Economic Research
and Policy Consulting
Kyiv 01030, Reytarska Str., 8/5-A
Tel. (+38044) 278-6342
Email: institute@ier.kyiv.ua
<http://www.ier.com.ua>

